DAVID L. ANDERSON (CABN 149604)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BRANDON CHARLES GLOVER, and VASILE MEREACRE, Defendants.	No. CR 18-00348 LHK VIOLATIONS: 18 U.S.C. § 1030(b) – Conspiracy to Violate 18 U.S.C. §§ 1030(a)(7)(B) and (c)(3)(A); 18 U.S.C. §§ 981(a)(1)(C), 1030(i), and 1030(j) – Criminal Forfeiture SAN JOSE VENUE

SUPERSEDING INFORMATION

The United States Attorney charges:

Introductory Allegations

At all times relevant to this Superseding Information:

1. Uber Technologies Inc. ("Uber") was a technology and transportation network company offering, among other things, ride service hailing. Uber was headquartered in San Francisco, California.

2. Lynda.com LLC was an online education company that offered video courses in software, creative, and business skills. On June 2, 2016, the company was acquired by LinkedIn Corporation ("LinkedIn"), which was headquartered in Sunnyvale, California.

3. "Bug bounty" programs are services wherein individuals that report security vulnerabilities receive recognition and compensation. Bug bounty programs assist companies in discovering and resolving security vulnerabilities so that they can be resolved before the general public is aware of them, thus preventing the wide-spread exploitation of the vulnerability.

4. LinkedIn maintained an invitation-only bug bounty program and accepted individuals, such as security researchers, into the program based upon the individual's reputation and previous work. LinkedIn established rules for participation in the program, and an individual would be disqualified from participation in the program based on a variety of factors, including making threats, demanding money in exchange for security vulnerabilities, publicly disclosing security flaws without notifying the company first, modifying, copying, downloading, deleting, or otherwise misusing other members' data, and accessing non-public member information without authorization.

5. HackerOne, headquartered in San Francisco, California, operated bug bounty programs for corporations, including LinkedIn and Uber.

6. Amazon Web Services was a subsidiary of Amazon, Inc. and headquartered in Seattle, Washington, that provided, among other services, cloud-based computing platforms.

7. GitHub, headquartered in San Francisco, California, was a cloud-based source code repository.

8. Uber maintained a bug bounty program that was administered by HackerOne.

9. Brandon Charles Glover ("GLOVER") was a resident of Winter Springs, Florida.

10. Vasile Mereacre ("MEREACRE") was a resident of Toronto, Canada.

COUNT ONE: (18 U.S.C. § 1030(b) – Conspiracy to Violate 18 U.S.C. §§ 1030(a)(7)(B) and (c)(3)(A))

11. The factual allegations at Paragraphs One through Ten are re-alleged and incorporated as if set forth fully here.

//

//

//

//

12. Beginning in approximately October 2016 and continuing to approximately January 2017, in the Northern District of California and elsewhere, the defendants,

BRANDON CHARLES GLOVER, and
VASILE MEREACRE,

did knowingly conspire and agree with persons known and unknown to the Grand Jury to commit an offense under 18 U.S.C. §§ 1030(a)(7)(B) and (c)(3)(A), that is, with the intent to extort from a person money and other things of value, transmitted in interstate and foreign commerce communications containing a threat to impair the confidentiality of information obtained from a protected computer without authorization.

Manner and Means

13. Defendants GLOVER and MEREACRE possessed and controlled and claimed to possess and control confidential databases and other data belonging to the victim-corporations all the while knowing that the data had been stolen from the victim-corporations' Amazon Web Services accounts. Using a cache of stolen user data, the defendants used their custom-built GitHub account checker tool to determine if the stolen data was also used as GitHub account credentials. The defendants then identified valid GitHub account credentials for corporate employees. They accessed several accounts belonging to the victim-corporations' employees and searched for Amazon Web Services' credentials. Once they found the Amazon Web Services credentials, they immediately used them to access the Amazon Web Services' Simple Storage Services, commonly known as S3, to search for and download sensitive data. The defendants exerted possession and control over the data in order to induce payments from the victim-corporations.

14. The defendants used the email address "johndoughs@protonmail.com" (hereinafter, the "johndoughs account") to contact the victim-corporations to report a security vulnerability and demand payment in exchange for deletion of the data. The defendants used false names to communicate with the victim-corporations, and, on several occasions, informed the victim-corporations that they had been paid by other victim-corporations for identifying security vulnerabilities. They also sent the victim-corporations a sample of the data in order for the victim-corporations to verify the authenticity of the data.

15. After examining the sample data, the victim-corporations communicated with the defendants about payment in exchange for the deletion of the data. In some instances, the victim-corporations referred the defendants to HackerOne for payment pursuant to the victim-corporations' bug bounty program. In other instances, the victim-corporation stopped communicating with the defendants and did not pay them for the data.

Defendants Extort Uber

16. As part of the conspiracy, defendants GLOVER and MEREACRE devised a plan to extort Uber by obtaining approximately 57 million records consisting of Uber customer data and Uber driver data from Uber's Amazon Web Services' S3 cloud-based data repository. The stolen data included drivers license information belonging to Uber drivers, and the names, email addresses, and telephone numbers of Uber customers.

17. On or about November 14, 2016, using the johndoughs account, the defendants contacted the Chief Security Officer at Uber and claimed to have "found a major vulnerability." In reality, the defendants had illegally accessed and downloaded approximately 57 million records of Uber customer data and Uber driver data. In addition, on or about November 14, 2016, Uber confirmed that a sample of the stolen data provided by the defendants in connection with the data breach did in fact contain Uber's confidential data.

18. The defendants demanded a minimum payment of $100,000, and Uber ultimately agreed to pay the defendants $100,000 in bitcoin, routed through its HackerOne account in order to classify it as a bug bounty payment.

19. In exchange for the payment of $100,000, Uber required the defendants sign confidentiality agreements prohibiting the use of the data and public disclosure of the breach.

Defendants' Plan To Extort LinkedIn

20. As part of the conspiracy, defendants GLOVER and MEREACRE devised a plan to extort LinkedIn by obtaining over 90,000 confidential Lynda.com user accounts from Lynda's Amazon Web Services S3 account, and exerting control over the accounts as a means to obtain money from LinkedIn.

21. The defendants used the johndoughs account to communicate with LinkedIn. They also

established an account with HackerOne using the false name "William Loafmann" and provided false information, such as names, addresses, and a Social Security number, on Internal Revenue Service forms.

22. On December 11, 2016, the defendants sent an email from the johndoughs account to the security team at LinkedIn notifying them about a "security flaw compromising databases of Lynda.com along with credit card payments and much more."

23. A LinkedIn executive responded a short time later requesting details so that LinkedIn could investigate the matter.

24. The defendants responded via an email sent from the johndoughs account, stating the following:

> Before I continue, I would like to say that this does not look good, I was able to access backups upon backups, me and my team would like a huge reward for this, [sic]. The things we found were some of the following, [L]ynda database, email names addresses, usernames, some passwords, payments, we also found backend code and many more. We also found partian [sic] [L]inkedin files. Before I continue, I would like to ask that you guys will promise to compensate for this find.

25. A LinkedIn executive and the defendants continued to communicate about the Lynda.com database, and the LinkedIn executive, in an attempt to identity the individual, lured the johndoughs account to join LinkedIn's bug bounty program through HackerOne.

26. After the invitation was extended, the defendants told the LinkedIn executive "[P]lease keep in mind, we expect a big payment as this was hard work for us, we already helped a big corp which paid close to 7 digits, all went well."

All in violation of Title 18, United States Code, Sections 1030(b), 1030(a)(7)(B), and (c)(3)(A).

FORFEITURE ALLEGATION: (18 U.S.C. §§ 981(a)(1) and 1030(i) and (j))

27. The factual allegations contained in Paragraphs One through Twenty-Six of this Superseding Information are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(1)(C) and 1030(i) and (j).

//

//

//

28. Upon conviction of the offense alleged in Count One of this Superseding Information, the defendants,

BRANDON CHARLES GLOVER, and
VASILE MEREACRE,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1030(i) and (j), any personal property used or intended to be used to commit or to facilitate the commission of said violation or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offense, including but not limited to, a sum of money equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from the violation.

29. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2).

All pursuant to Title 18, United States Code, Sections 981(a)(1) and 1030(i) and 1030(j).

DATED: 10/30/19

DAVID L. ANDERSON
United States Attorney

SUSAN KNIGHT
AMIE D. ROONEY
Assistant United States Attorneys

AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☒ INFORMATION ☐ INDICTMENT
☒ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

FILED
OCT 30 2019
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE
9:03 AM
SUSAN Y. SOONG

OFFENSE CHARGED

COUNT ONE: 18 U.S.C. § 1030(b) – Conspiracy to Violate 18 U.S.C. §§ 1030(a)(7)(B) and (c)(3)(A); 18 U.S.C. §§ 981(a)(1)(C), 1030(i), and 1030(j) – Criminal Forfeiture

☐ Petty
☐ Minor
☐ Misde-meanor
☒ Felony

PENALTY: 5 years imprisonment, $250K fine, 3 years supervised release, $100 special assessment.

DEFENDANT - U.S

▶ BRANDON CHARLES GLOVER

DISTRICT COURT NUMBER
CR-18-00348 LHK

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)
S/A Jeff Miller and Jon Chinn, FBI

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:
☐ U.S. ATTORNEY ☐ DEFENSE
} SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under
} MAGISTRATE CASE NO.

DEFENDANT

IS *NOT* IN CUSTODY

1) ☐ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges ▶

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges
If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☐ No } If "Yes" give date filed

DATE OF ARREST ▶ Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year

Name and Office of Person Furnishing Information on this form DAVID L. ANDERSON
☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) SUSAN KNIGHT

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:
☐ SUMMONS ☒ NO PROCESS* ☐ WARRANT Bail Amount:
If Summons, complete following:
☐ Arraignment ☐ Initial Appearance
Defendant Address:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Date/Time: Before Judge:

Comments: